Secure SD-WAN / SD-Branch (Fortinet)

Service Definition

Version 1.0
November 2024

redcentric

AGILE • AVAILABLE • ASSURED

1) Service Overview

1.1) Introduction and overview

Redcentric's Secure Software Defined-Wide Area Network (SD-WAN) Service using Fortinet firewalls is designed to complement traditional private IP-VPN networks. It allows customers to make optimum use of the available bandwidth at their sites, and to supplement private connections with cellular, low-cost internet and other links. Application visibility, control and performance can be enhanced, delivering greater levels of efficiency and user satisfaction.

When Secure SD-WAN technology is integrated with other network elements, such as LAN and WLAN, it brings the most secure and manageable remote branch in the industry – Secure SD-Branch. Secure SD-Branch comprises of FortiGate Secure SD-WAN, FortiSwitch and FortiAP.

1.2) Key features and benefits

Redcentric Secure SD-WAN/SD-Branch based on Fortinet products offers several key differentiators over competitive options:

- It enables security-driven networking by using the FortiGate next-generation firewall (NGFW).
- SD-Branch consolidates networking and security capabilities into a single solution that provides seamless protection of distributed environments.
- It uses Fortinet Security Fabric architecture to extend security throughout the network access layer to include FortiAPs (secure wireless access points) and FortiSwitch with FortiLink (secure Ethernet).
- Single-pane-of-glass management of security, network access, and SD-WAN using a common centralised management platform called FortiManager.
- Security engrained into the network from the start.
- Zero Touch Provisioning (ZTP) / Low Touch Provisioning (LTP). This enables large scale, faster deployment of Secure SD-WAN and SD-Branch.
- Application resilience – Ensures the highest level of application availability and performance over any WAN transport.

2) Service Description

2.1) Associated Products and Pre-requisites

The SD-Branch/SD-WAN Service is designed to augment Redcentric's Managed IP-VPN/DIA services portfolio. Together they represent hybrid WAN, offering a combination of unbeatable features – robust end-to-end assurance and SLA where required, plus cost-effective improvement to application performance.

2.2) Service Overview

Typically, a SD-Branch solution consists of a SD-WAN FortiGate firewall, a FortiSwitch and a FortiAP.
A FortiManager is mandatory when deploying a managed SD-Branch.

The SD-WAN topology depends on the customer requirements and will be deployed accordingly. When multiple sites are required, and edge to edge or edge to data centre communication is needed, a Hub-and-Spoke topology will be employed. For smaller deployments where the above elements are not necessary, but the site still benefits from at least two WAN links, a far simpler deployment is available that still employs the advantages of SD-WAN.

The following diagram depicts the elements that make a typical SD-Branch.

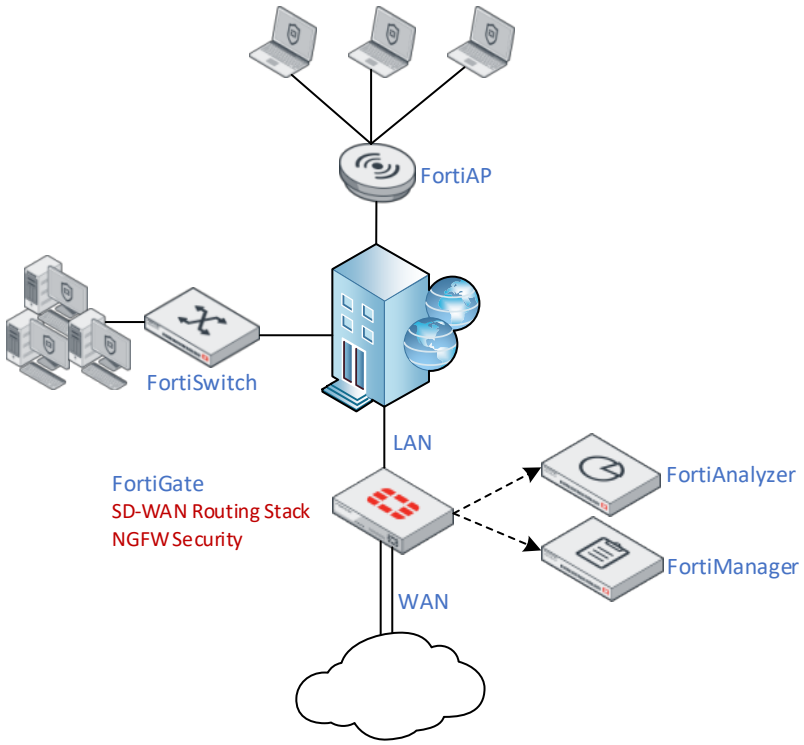

Diagram 1: Redcentric SD-Branch components

Component	Description
FortiGate	NGFW provides edge security with full visibility and threat protection. SD-WAN Routing Stack
FortiSwitch	Secure, simple, and scalable Ethernet switches for wired LAN network requirements
FortiAP	Secure and scalable Wireless (Wi-Fi) services
FortiAnalyzer	Provides security fabric analytics and automation to provide better detection and response against cyber risks through the collection of logs from all Fortinet devices within the security fabric
FortiManager	Centralised management platform for SD WAN and SD-Branch, delivering unified management capabilities for consistent configuration and security policies across complex hybrid environments resulting in protection against security threats.

FortiGate

Available in all form factors, including physical and virtual appliances, the FortiGate firewall delivers fast, scalable, and flexible Secure SD-WAN on-premises and in the cloud.

As standard, firewall policies with internet traffic will be configured with AV, IPS, App Control, Web Filter, where policies with traffic destined for internal systems would be configured with AV and IPS.

As standard, Firewall policies Log Allowed Traffic will be set up as Security Events only.

FortiGate firewalls are pre-configured with a 'default' security profile. As standard, a custom security profile will be created as a clone to the existing 'default' profile.

AV – default

- Default action: **Block**
- Inspected Protocols: HTTP, SMTP, POP3, IMAP, FTP
- APT Protection Options:
  - Treat windows EXE in email attachments as viruses: **Enabled**
  - Include mobile malware protection: **Enabled**

Web Filter – default

- Feature set: Flow-based
- FortiGuard Category Based Filter:
  - **Blocking**: Potentially Liable (Child Sexual Abuse, Crypto Mining, Potentially Unwanted Programs, Terrorism), Adult/Mature Content, Security Risk, Unrated
  - **Monitoring**: Potentially Liable (Drug Abuse, Hacking, Illegal or Unethical, Discrimination, Explicit Violence, Extremist groups, Proxy Avoidance, Plagiarism)
  - **Allow**: Bandwidth Consuming, General Interest – Personal, General Interest – Business

Application Control – default

- Default Action – **Monitor** all applications
- **Allow** – Unknown Applications

IPS – Custom Internet Access

- Prevents critical attacks
- IPS Signatures and Filters
  - Type: Filter
  - Action: Default
  - Packet logging: Disable
  - Status: Default
  - Filter: Severity (Medium, High, Critical), OS
- Botnet C&C
  - Scan Outgoing Connections to Botnet Sites: **Block**

IPS – Custom Corporate Access

- Prevents critical attacks
- IPS Signatures and Filters
  - Type: Filter
  - Action: Default
  - Packet logging: Disable
  - Status: Default
  - Filter: Severity (Medium, High, Critical), OS
- Botnet C&C
  - Scan Outgoing Connections to Botnet Sites: **Disable**

IPS default action selection criteria explained:

Fortinet's IPS signatures have two main actions – 'Pass' or 'Block'. Ideally, all signatures have a default block action. However, due to the dynamic nature of network environments and vulnerabilities, it is difficult to avoid false positives or to assess which vulnerability is more severe in an environment. Signatures are set up such that a user can easily modify the action to suit their needs.

Even though every new IPS signature must go through the Beta-Testing stage before official release, it is always released to the public with its default action set to 'Pass'. This is because a good balance of a well written

signature is needed, and a quick response rate to mitigate the attacks for all customers as soon as possible. After the official release, Fortinet will further monitor and evaluate the signature for a period of time, upon which, the signature will be reviewed to determine if its default action must be modified. How to determine the default action of a signature then, is not only by the severity of the vulnerability, but by a few different factors. The selection criteria for signatures with default action block is an aggressive one. The main reason is that security is valued as the number one priority to the customer.

The criteria are as follows:

1) The signature is for coverage of a vulnerability targeting a popular application.

2) The signature is for coverage of a known exploit in the wild.

3) The signature has low risk of false positives.

With the criteria above, over 90% of the signatures have the block action. With such aggressive criteria, there will be a possibility of missing some attacks or blocking some legitimate traffic.

This is why Fortinet goes through a stringent process of testing, evaluating, and reviewing signatures before these are released and with their action switched from pass to block. Where the signature does not meet the criteria above, its default action will be set to 'Pass'.

IPS status default explained:

The IPS signature list has redundant, obsolete, or false positive signatures. These signatures are assigned to a default value of enable or disable. The IPS sensor configuration "default status" is defined by the FortiGuard IPS Team and is updated regularly depending on the signature, monitor results etc. The FortiGate GUI or FortiManager should not change the status at all because it negates any intelligence added by the FortiGuard team to reduce false positives or unwarranted network disruptions due to IPS signatures.

Resource and research are available at: https://www.fortiguard.com/

As standard, in a Hub-and-Spoke topology, SSL Certificate Inspection will be enabled on the Edge firewalls. SSL Deep Inspection will be enabled on Hub devices, as well as any Edge device deemed as a Super-Spoke (i.e. Headquarter with various services).

For maximum security, using SSL deep inspection is required if all traffic is to be analysed or protected. Encrypted traffic might miss IPS and AV analysis if deep inspection is not used.

- If Web Filter only is required, SSL Certificate Inspection is the recommended option.
- If Web Filter, IPS, AV and Application Control are required, then SSL deep inspection is the best option.

FortiSwitch

A FortiGate managed FortiSwitch deployment using FortiLink is the most common deployment and doesn't require an additional license.

Managing the FortiSwitch using a FortiGate offers the following:

- Zero-touch provisioning: FortiSwitch only needs connected to a FortiGate interface that has FortiLink enabled. The FortiGate automatically discovers and provisions the switch.
- Secure configuration management: All configuration is done via the FortiGate/FortiManager GUI and CLI, removing the requirement to log into the switches.
- Centralised provisioning and maintenance: FortiGate or FortiManager is the single point of management, to include but not limited to auto-discovery, authentication, and authorisation, vlan provisioning, policy deployment.
- FortiSwitch stack: FortiGate can manage multiple FortiSwitch devices stacked in different.

Intra-vlan traffic is handled by the switch/stack and any other traffic is handled by the FortiGate.

As standard, switches will be deployed using central management mode from the FortiManager. Central management mode employs a single configuration for all switches. A single FortiSwitch template per platform will be created. Where available, the default built in template objects (LLDP profiles, QoS Policies) will be used.

Per-device management mode (settings and profiles are applied to individual FortiSwitch devices, that enables you to deploy sites that use different configurations) is also available – subject to additional charges.

FortiAP

As standard, Redcentric will deploy the FortiAP in a direct connection deployment mode (direct connection to the FortiGate Wi-Fi controller) and/or in a switched connection deployment mode where the FortiAP is connected to the FortiGate Wi-Fi controller via a FortiSwitch. A mesh deployment is also available where required – subject to caveats/limitations.

Like the FortiSwitch deployments, two modes are available: central management and per-device management. As standard, central management mode will be employed using shared Wi-Fi profiles to deploy configuration to controlled APs. Changes made on a Wi-Fi profile result in a configuration change on multiple APs. As standard, a single Wi-Fi profile specific to a FortiAP model will be created.

In per-device management mode the FortiManager maintains a set of Wi-Fi profiles for each wireless controller (FortiGate), instead of having a set of profiles that are shared among all APs controlled by all FortiGate devices - available - subject to additional charges.

A Radio Frequency (RF) coverage plan is produced using Customer provided location plans of the areas of the building(s) where WLAN coverage is required. The individual components required to deliver the Service including specific model(s) of Access Point (AP) and any centralised authentication infrastructure are derived from specific Customer requirements for each site.

The initial design is based on the following customer supplied information:

- Location floor plans
- Details of internal features (wall type)
- Anticipated user density
- Required services (E.g. Data, Voice, Guest Internet access etc.)
- Security requirements including WLAN encryption and authentication methods
- Radio coverage and system redundancy requirements
- Details of Internet access where Redcentric is not providing Wide Area Network connectivity
- External factors such as interference and building construction can affect the wireless coverage.

Customers can select optional site surveys which generally results in a design more likely to meet any Radio Frequency (RF) coverage requirements, and without a site survey the design is less likely to provide optimum coverage.

Redcentric produces initial desktop designs based on industry best practice by applying the following design principles by default:

- For data only wireless, Redcentric will propose AP coverage overlap of 15% and no resilient AP visibility.
- For data only wireless where a level of resilience is required, Redcentric will propose AP coverage overlap of 15% per cell with visibility of 1 additional AP at -75dBm.
- For voice/video (e.g. real-time traffic), Redcentric will propose AP coverage overlap of 20% per cell with visibility of at least 2 APs at -67dBm.

As standard, two WLANs will be deployed:

- **Corporate Wireless LAN** – Connection to the Corporate LAN will be provided using a dedicated SSID which can be broadcast from all or a sub-set of the access points on the managed wireless network. Authentication and authorisation of corporate users and/or devices will be achieved using a RADIUS server and an authentication credential store such as the corporate Active Directory or a compatible LDAP compliant server (Customer or Redcentric supplied)

- **Guest Internet Access Wireless LAN** – The basic Managed WLAN Service enables the Customer to provide a basic Guest Internet access capability to its visitors, via a dedicated SSID.

FortiAnalyzer

FortiAnalyzer is a powerful log management, analytics and reporting platform that provides organisations with a single console to manage, automate, orchestrate, and respond, enabling simplified security operations, proactive identification and remediation of risks, and complete visibility of the entire attack landscape.

Logs in FortiAnalyzer are in one of the following phases:

- **Real-time log**: Log entries that have just arrived and have not been added to the SQL database. These logs are stored in Archive in an uncompressed file.
- **Archive logs**: When a real-time log file in Archive has been completely inserted, that file is compressed and considered to be offline. When FortiAnalyzer receives a log, it is stored in a file. Logs will continue to populate this file until its limit is reached, at which time the file is "rolled", which involves compressing the file and creating a new one for further logs of that type. These files (rolled or otherwise) count against the archive retention limits and are referred to as Archived or Offline logs. Archive logs are stored unchanged and can be uploaded to a file server for use as backups.
- **Analytics logs**: Indexed in the SQL database and online. Immediately following the storage of a log in an archive, the same log is inserted into the SQL database. This function is also known as being indexed, and these logs are referred to as Analytic or Online logs. Analytic logs are dissected during insertion and any subtypes are stored as their own category.

In a conventional FortiAnalyzer, logs are stored in two different formats:

- **Archive logs**: offline logs used for log retention only
- **Analytics logs**: online logs indexed in SQL database and available for analytical support (FortiView, Reports, etc.)

    - The following table provides the average log size per log storage format. By default, analytics logs older than 7 days are compressed. This makes them slower to retrieve, read, and display, but much more storage efficient.

Format	Size
Archive Log	80 bytes
Analytic Log – Uncompressed*	600 bytes
Analytic Log – Compressed*	150 bytes

Redcentric uses the following formulas to approximate the storage required for the FortiAnalyzer appliance. The figures below are used as guidance only and are **per device. These will be subject to change post install.**

Archive size per day = 3logs/sec*80bytes*86400 seconds = 0.019GB/day – 7GB/365 day

Analytics compressed per day = 3logs/sec*150bytes*86400 seconds =0.036GB/day – 2.16GB/60 days

Analytics uncompressed per day = 3logs/sec*600bytes*86400 seconds = 0.15GB/day – 1.05GB/7 days

Redcentric provides two different offerings depending on customer needs:

- Shared FortiAnalyzer
    - Dedicated ADOM (Administrative Domain)
    - Secure Access to the Customer ADOM portal

- Dedicated FortiAnalyzer
    - When a Customer requires log forwarding to 3dr party SIEM
    - When a Customer intends to backup logs via SFTP with a custom roll log file size
    - When a Customer requires greater than the default log analytic and archival settings
    - As standard, a dedicated FortiAnalyzer will be located within Redcentric IaaS. Access to the FortiAnalyzer portal is done via the Hub firewall devices; a dedicated virtual firewall located within Redcentric datacentre is an alternative solution to secure and access the FortiAnalyzer – subject to additional charges.

FortiManager

As standard, a dedicated ADOM on a shared FortiManager, per customer will be configured. For customers requiring management access to their estate via the FortiManager, secure access using MFA (multi-factor authentication) is available – (subject to caveats and prior agreements).

For Customers with a dedicated FortiManager, Redcentric offers two options:

- Using a Redcentric Virtual Firewall – The Customer FortiManager is protected by a virtual firewall maintained by Redcentric (additional charges apply for both the firewall and Redcentric FortiManager).
- Using the Customer Hub Firewall – Securing the Customer FortiManager through the Hub firewalls is contingent upon a written agreement. If this preference is chosen, it becomes the Customer's responsibility to ensure continuous access to the Customer FortiManager. Should alterations to the Hub firewalls lead to difficulties accessing the FortiManager, Redcentric reserves the right to impose additional charges to address the issues.

2.3) Variants: functionality included/excluded deliverables/limitations

- Custom FortiGate UTP profiles are available – subject to additional charges.
- Access to the FortiAnalyzer and FortiManager portal for customers with shared appliance to their respective ADOM has MFA (multi-factor authentication) support.
- Access to the FortiAnalyzer and FortiManager portal for customers with dedicated appliances has no MFA support. Access is done via a dedicated virtual firewall or Hub firewall, either from the customer network or externally via a VPN solution.
- Limited scope for deploying devices internationally.
- The level of Hardware Support must be the same for all Customer locations. E.g. ALL sites: 12 hour fix.
- There is a limit of APs that can be managed by a FortiGate depending on the model.
- Wi-Fi mesh deployment comes with disadvantages such as hop count that affects latency, availability etc.
- Read-Write rights to the FortiManager ADOM is subject to prior written agreements.

2.4) Licensing

As standard, all FortiGate devices will be licensed for Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium).

FortiSwitch and FortiAP do not require a separate license, however there is FortiCare Premium and Elite support.

FortiAnalyzer and FortiManager require licensing. A Redcentric representative will discuss this according to the Customer needs.

2.5) Service Implementation

A Redcentric Project Manager will engage with the Customer and outline the approach for delivery including any customer specific information, resource or access needed prior to deployment.
The Project Manager coordinates procurement/ordering, configuration, deployment, testing and hand-over tasks. In most cases, the service is installed by a Redcentric engineer.

A pre-requisite to deployment is a technical information gathering exercise. Information required to deploy the Service includes but is not limited to the following aspects:

- Technical details of 3rd-party connections – IP addressing, DHCP servers etc.
- Applications – priorities & performance parameters
- Firewall security policy and other security parameters
- SD-WAN routing requirements
- Precise address, floor, room & location of circuit termination and CPE location
- Contact details for report recipient(s)

2.6) Customer Responsibilities

The Customer is responsible for all other aspects including but not limited to the following:

- Define SD-WAN rules and policies
- Define firewall rule base and other security parameters
- Define users and DNS configuration
- Provide Redcentric with an up-to-date list of staff authorised to submit change requests
- Report and manage faults directly with connectivity suppliers other than Redcentric
- Provide Redcentric technical and admin details required for delivery
- Preparation of Local Area Network as required.
- Install any software required as per solution.

- The Customer Corporate Wireless LAN and Guest Internet Access Wireless LAN services (together "WLAN Services") will be provided to end users by the Customer
- The Customer will be responsible for all user management in relation to the WLAN Services
- The WLAN Services are set up in such a way that each end user must accept the Customer's end user licence agreement (EULA) before being able to access the service. The WLAN Services are provided with a simple and generic EULA between the Customer and the end user. The generic EULA will not be suitable for the Customer's business, and the Customer must amend the EULA to suit its own requirements (as explained in, and subject to, the legal agreement between Redcentric and the Customer).
- Charging for the basic service does not include any structured cabling checks, cable work or patching between switch and structured wiring frames. If the FortiGate firewall terminating the circuit(s) and the managed switch are within one metre of one another, the Redcentric engineer will provide patch cable(s) to connect them together. Upon request, Redcentric will undertake a general or detailed survey of existing structured cabling and provide a report on its suitability for certain applications. Redcentric can arrange for cabling to be upgraded, repaired, corrected, extended, tidied, re-patched, labelled and replaced as required to ensure a Customer's entire LAN is fit for purpose (e.g. to support IP telephony). This work is chargeable and priced on application.

2.7) Redcentric Responsibilities

Redcentric staff are responsible for the following aspects:

- Service design based on information supplied by the Customer
- Configuration of the FortiGate firewall, FortiSwitch and FortiAP devices and the associate systems (to include FortiAnalyzer, FortiManager)
- Physical installation / deployment of devices on Customer locations when optionally chosen (additional charges may apply) – explicit up-front agreement in writing by both parties prior to finalising a Service Agreement
- Provide required software
- Organize replacement of faulty hardware
- Upkeep / upgrade / patching of management, reporting & appliance
- Alerting platforms
- Notify Customer of 3rd party connectivity issues
- Provide LLD documentation

2.8) Monitoring

Redcentric polls the service elements of the solution and retrieves information relating to:

- System parameters (e.g., CPU utilization, storage, and memory usage)
- Environmental parameters (e.g., Temperature and Voltage)
- Connectivity failures
- Live configurations
- Configuration changes
- Availability monitoring (icmp, port scans)
- Delay, jitter and packet-loss characteristics on SD-WAN links

- The following parameters must be configured, monitored, and defined alerts acted on (subject to change in agreement with Support Services):

SD-WAN		DataPoint	Description	Action
	BGP	PeerState	The BGP peer connection state. 1 = idle; 2-5 Connecting; 6 = Established.	<>6 for > 120seconds then: Major
	IPSec tunnels	Status	Current status of the tunnel. Status codes: 1=Down, 2=Up	=1 for >120 seconds then: Major
	SDWAN Performance SLA	Jitter	Average jitter on the specified SD-WAN link.	> 30mS if sustained > 5min: Major
		Latency	Average latency, in milliseconds.	1way > 150mS (or RTT > 250mS) if sustained > 5min: Major
		Packet Loss	Packet loss in percent.	> 1% if sustained > 5min: Major

- The above settings are not to be confused with the Performance SLA configurable in the SD-WAN template. Due to the nature of the SD-WAN behaviour, in the event of blackout/brownout situation a failover trigger may be activated. It is not expected that every such failover will be investigated, as this could be due to the nature of the circuit (i.e. broadband and expected packet loss). However, if such an event does not clear itself within the given parameters above, it is expected this is investigated as per the severity of the alert.

The platform is configured with threshold values and quell-times for each of the attributes listed above.
If the measured values cross the threshold and stay that way beyond the quell-time, the system automatically triggers an event in the Redcentric Service Management application and a service ticket is generated and assigned.

2.9) Incident Management

When an event is triggered or identified and validated by a member of the Redcentric support team, a fault ticket is raised. Tickets are managed by engineering professionals in Redcentric's operations centre 24/7/365.
If the issue relates to the SD-WAN/SD-Branch Service or a Redcentric supplied circuit, Redcentric is responsible for managing the fault through to resolution.

If the issue relates to an element not supplied by Redcentric, Redcentric will notify the Customer contact in accordance with the Customer Welcome Pack. Redcentric does not deal with customers 3rd party suppliers directly.

2.10) Hardware Maintenance and Support

Please refer to the System Maintenance section with Infrastructure as a Service (redcentricplc.com) for the supporting IAAS details.

2.11) Maintenance Notice and Scheduled Downtime

To provide a robust service, Redcentric occasionally performs upgrade and maintenance tasks on systems and platforms. Details of maintenance windows and how they are communicated are detailed in Redcentric's Customer Welcome Pack and Master Service Agreement documents, which should be read in-conjunction with this document.

2.12) Change Notice

Redcentric occasionally updates and improves services and adds new features as it strives to provide Customers relevant and valuable services. The Redcentric Master Service Agreement details the implications of Service Change and how it will be communicated.

2.13) Changes

Redcentric support staff manage the configuration of the solution components, evaluating and implementing formal change requests submitted by the Customer.

In accordance with the Redcentric change request procedure, all change requests must be submitted by a designated and authorised Customer technical contact. If Redcentric's security engineer cannot validate the change requester against the authorised list, then Redcentric will place the change request on hold and attempt to contact one of the alternative authorised contacts. Redcentric must wait for the request to be ratified by a known authorised contact before proceeding with any firewall change. It is therefore essential that Customers provide accurate and current contact information for their designated and authorised staff.

It is extremely easy to weaken network integrity and/or security by submitting a seemingly innocuous change request. Redcentric staff review change requests based only on the information they have available, and therefore Redcentric cannot take responsibility for network weakness resulting from rule-base changes. If Redcentric support staff believe that a rule-base change request compromises the security of the Customer's network, Redcentric may ask the Customer to sign a disclaimer stating that they wish to go ahead regardless of the advice offered.
In extreme cases, staff reserve the right to reject the change outright; for example, if the weakness could affect other Redcentric Customers.

2.14) Reporting

Customers are provided with secure access to the FortiAnalyzer for reports and monitors. FortiAnalyzer includes a library of default report templates that will be available as standard. Please note that not all the available templates will be of use to customer as they cover an extensive range of Fortinet products.

Additional tailored reports can be made available at additional charge.

3) Implementation and Acceptance

3.1) Acceptance Criteria

Acceptance Criteria applicable to the SD-WAN/SD-Branch Service are listed below:

SD-WAN/SD-Branch Service	Service Availability
IAAS Server Solution	≥99.99%
Portal access	≥99.5%

- Confirm Redcentric Support contact details have been supplied
- Check the LAN connections to the End Point Devices device(s) for speed and duplex mismatches and errors (where possible).
- Test IP connectivity by using permitted protocol traffic from permitted devices on each interface destined for permitted addresses on the other interfaces (e.g. test traffic on port 80 from a device on the internal network destined for a server on the outside network)
- Test the functionality and notification mechanisms of the service
- Provide Customer access to the Service Portal

4) Service Levels and Service Credits

4.1) Service Levels

Service Levels for the Redcentric SD-WAN/SD-Branch Service elements are detailed in the table below.

Service Levels for underlying connectivity provided by Redcentric is detailed in the applicable Service Definition.

SD-WAN service element	Service availability
Single SD-WAN spoke or hub appliance on a customer site	≥99.0%
Single SD-WAN hub appliance located in a Redcentric data centre	≥99.5%
Portal access for analysis and visibility etc.	≥99.5%

4.2) Exclusions from Availability

In calculating Availability, in addition to the exclusions listed in clause 6.7 of the General Terms the following shall be excluded:

- Unavailability due to tasks required to implement and test change requests.
- Unavailability due to malicious activity of any kind. E.g., a Denial-of-Service attack (DOS)
- Unavailability due to hardware failure when only a Single Server Solution is deployed.
- Failure of site connectivity which prevents measurement of service components availability.

4.3) Floor Service Level

The Floor Service Level applicable to the Redcentric SD-WAN/SD-Branch Service in respect of Availability shall be 85% in any given Month.

4.4) Service Credits

The Service Credits applicable to the SD-WAN/SD-Branch service shall be calculated as follows.
In the following table:

“≥” means “greater than or equal to”
“<” means “less than”
“MS” means the Charges payable in respect of the SD-WAN/SD-Branch service for the same Month for the effected site(s)

Applicable SD-WAN/SD-Branch service	Service Availability	Service Credit
IAAS Server Solution	≥99.99.%	none
	≥99.98.% but <99.5%	5% of MS
	≥99.49% but <99.0%	15% of MS
	<99.0%	20% of MS
Portal Access	≥99.5%	none
	≥99.0% but <99.5%	1% of MS
	≥99.5% but <97.0%	2% of MS
	<97.0%	5% of MS

5) Data Processing

5.1 Data Processing Scope

- Redcentric’s SD-WAN/SD-Branch Service delivers a degree of IP network perimeter protection.
- Redcentric’s SD-WAN/SD-Branch Service may involve the storage of summarised traffic and user activity.

5.2 Data Storage and Encryption

- Devices may be configured to encrypt traffic across certain networks.
- By the very nature of the Service, it is necessary for Redcentric to capture, inspect, analyse, and store the Customer’s traffic/data.
- Redcentric would not have access to the content of the Customer’s traffic/data in normal circumstances. Under certain circumstances, when managing a support ticket, Redcentric may further capture, inspect, analyse and/or store samples of the Customer’s traffic in order to investigate and diagnose specific problems. Such actions will only be undertaken at the request of and in conjunction with the Customer.
- The period for which data is stored in relation to the Redcentric SD-WAN/SD-Branch Service is decided by the Customer.

5.3 Data Processing Decisions

- Redcentric does not make any data processing decisions in relation to the Redcentric SD-WAN/ SD-Branch Service. Any processing of data over Customer systems when using the Redcentric SD-WAN/SD-Branch Service is instigated, configured and managed by the Customer.
- Redcentric Support can be asked by the Customer to intervene in the event of an issue with the Redcentric SD-WAN/SD-Branch Service. In such a case Redcentric may make decisions that affect data processing, but such actions will only be undertaken at the request of and in conjunction with the Customer.

5.4 Sub-processors

- Redcentric's SD-WAN/SD-Branch Service may make use of services provided by the selected hardware vendor (E.g., Fortinet, Cisco Systems etc.). These services assist with the identification of security vulnerabilities, weaknesses, exploits, virus, worms etc.
- No other parties are involved in delivering the Redcentric SD-WAN/SD-Branch Service, and no other sub-processors are appointed by Redcentric.

5.5 Customer Access to Data

The Customer controls its own platforms which use Redcentric's SD-WAN/SD-Branch Service, and the Customer therefore has full access to its own data.

5.6 Security Arrangements and Options

The Redcentric SD-WAN/SD-Branch Service may be hosted at both Redcentric and third-party locations.
All Redcentric appointed locations meet physical security standard ISO 27002 section 11.1

END OF DOCUMENT

HEAD OFFICE

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522
E sayhello@redcentricplc.com
W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED